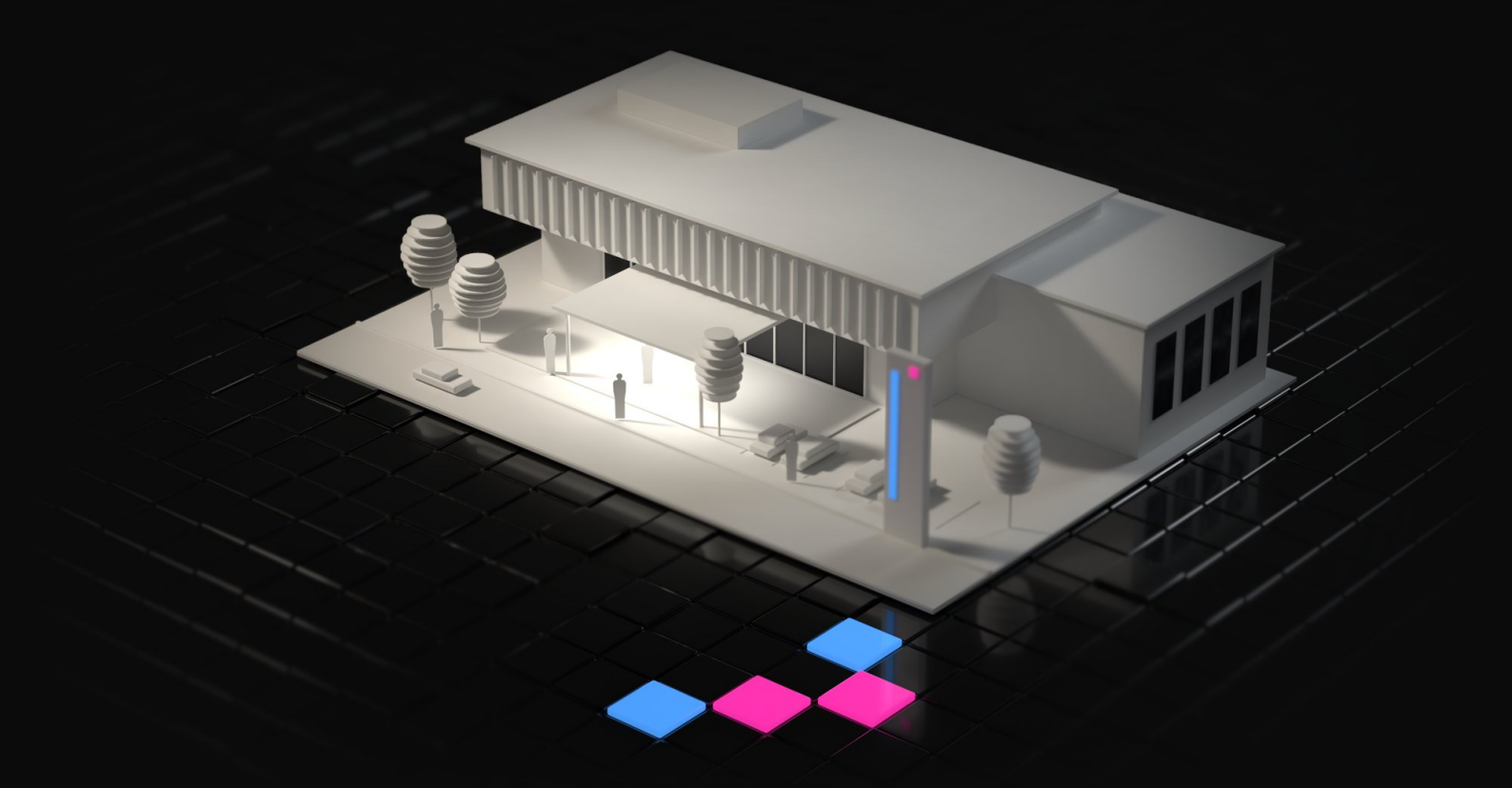


FOR STAFF · AS OF NOVEMBER 2026

Working from home. Simplified.

Simple rules for staff working from home or on the road, without slowing anyone down.

John Morgan · Initial Technology · November 2026

THE ONE THING TO KNOW

Home is fine. Home habits are the risk.

Working from home is safe when the device is looked after, the files stay in the club's systems, and people are a little more careful about who's listening.

SIMPLIFIED

Club device, updated and locked. Files in OneDrive or SharePoint. Home Wi-Fi with a strong password. Lock the screen.

FIVE THINGS AT A GLANCE

01

Look after the device

Club-managed, updated, encrypted.

02

Secure the Wi-Fi

Strong password, router updated.

03

Keep files in the club's systems

Not on USBs or personal email.

04

Lock it when you leave

Even for a coffee.

05

Watch who's listening

Calls, screens and printouts.

06

Approve only what you started

Never accept a sign-in prompt you didn't start.

STEP 01

The device

The single biggest factor.

- [ ] **Use a club device.**
  Managed with Intune, encrypted, with a remote wipe.
- [ ] **Screen lock after five minutes.**
  And a passkey or fingerprint to unlock.
- [ ] **Updates on, and restart weekly.**
  Most updates need a restart to work.
- [ ] **Personal phones for email only if managed.**
  Microsoft's app protection keeps club data separate.

STEP 02

The home network

Ten minutes, once.

- [ ] **Change the router's admin password.**
  Not the one on the sticker.
- [ ] **Update the router.**
  Or replace it if it's more than five years old.
- [ ] **Use WPA3, or WPA2 at least.**
  With a strong Wi-Fi password.
- [ ] **Use your phone's hotspot in public.**
  Not café or hotel Wi-Fi.

HANDY TIP

A separate guest Wi-Fi at home keeps the kids' gaming console and smart TV off the same network as the work laptop.

STEP 03

The files

If it's not in the club's systems, it's not backed up or protected.

- [ ] **Save to OneDrive or SharePoint.**
  Not the desktop, a USB or personal Dropbox.
- [ ] **Don't print member or staff details at home.**
  If you must, shred them.
- [ ] **Don't email files to yourself.**
  Share a link instead.
- [ ] **Report a lost device straight away.**
  It can be wiped remotely.

WRITE IT DOWN

WHO TO CALL IF A DEVICE IS LOST _____

STEP 04

Calls and screens

The low-tech risks.

- [ ] **Board and HR calls somewhere private.**
  Smart speakers and family can hear.
- [ ] **Lock the screen when you step away.**
  Windows key + L.
- [ ] **Blur or set a background.**
  Whiteboards and paperwork show on camera.
- [ ] **Check who's on the call.**
  Unknown attendees on sensitive meetings get removed.

Want this set up properly for your team?

I'll check your device management, sharing settings and home-working policy, and give staff a one-page guide they'll actually read.

0401 539 456 · info@initialtech.com.au · initialtech.com.au

THE SIMPLIFIED GUIDES

Free at initialtech.com.au/resources

01 Microsoft 365 security
02 Cyber basics and phishing
03 Ransomware readiness
04 Backup and recovery plan
05 Incident response
06 Working from home securely
07 Copilot readiness
08 Choosing an IT provider
09 Buying a major system
10 The board technology report
11 Copilot vs ChatGPT vs Claude

Sources, checked November 2026. ASD's ACSC: Small business cyber security guide; Securing your home network; How-to guides for Microsoft devices and accounts. Microsoft: Intune app protection policies. General information only, not legal, insurance or financial advice. Check current details with your IT provider before acting.